Microsoft Exchange Server

Chapter 4
Connecting Active Directory to Exchange 5.5

Planning Guide

Abstract

If you need to operate a mixed Exchange 5.5 and Exchange 2000 site, you will need a mechanism for synchronizing the two directories. This chapter takes you through the process of designing a link between Exchange 5.5 and the Windows 2000 Active Directory. After going through this process, you will have all the information necessary to plan the implementation of this type of connection within your organization.

This is a preview edition of the Microsoft Exchange 2000 Server Upgrade Series. The final documentation will be available in November 2000.

© 2000 Microsoft Corporation. All rights reserved.

THIS IS PRELIMINARY DOCUMENTATION. The information contained in this document represents the current view of Microsoft Corporation on the issues discussed as of the date of publication. Because Microsoft must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Microsoft, and Microsoft cannot guarantee the accuracy of any information presented after the date of publication.

This document is for informational purposes only. MICROSOFT MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS DOCUMENT.

Microsoft, Active Directory, Windows, Windows NT and the Windows logo are registered trademarks of Microsoft Corporation.

Other product or company names mentioned herein may be the trademarks of their respective owners.

Microsoft Corporation • One Microsoft Way • Redmond, WA 98052-6399 • USA

1000

CONTENTS

INTRODUCTION....1
Exchange 5.5 and Active Directory 1
Architecture and Design Phases 1
Windows 2000 Active Directory 2
Resource Requirements 2
Personnel 2
Security and Account Privileges 3
Skills 3
Hardware, Software and Logistics 3
Planning Prerequisites 4

PROCESS FLOWCHART....5

PLAN AND DEPLOY ACTIVE DIRECTORY....6

REVIEW EXCHANGE 5.5 ENVIRONMENT....8

PLAN ACTIVE DIRECTORY CONNECTOR....9
How ADC Works 9
ADC Versions 9
Architecture Strategy 10
Related Topics 13

PLAN FOR SCHEMA EXTENSION....14

Summary....15

INTRODUCTION

This chapter takes you through the process of planning for the connection of your Exchange 5.5 directory to the Active Directory. You will not be covering the process of planning for the Active Directory itself; however, you will be told what Active Directory issues you need to consider if you have Exchange 5.5 and you are upgrading to Exchange 2000. In addition, this chapter will look at the Active Directory Sizing Tool (AD Sizer), which allows you to plan server size and capacity based on a number of input parameters regarding your Exchange environment.

This chapter assumes that you have a fully functional Active Directory already deployed. Information on planning for the Active Directory is available in the Windows 2000 Deployment Planning Guide.

Exchange 5.5 and Active Directory

Exchange 5.5 has its own directory service, which is independent of the operating system. This means that mailboxes, distribution lists and other objects are stored in a separate repository from the users' system account information.

This system has changed completely with Exchange 2000 and Windows 2000, which both share the same directory service. This means that Exchange 2000 and Windows 2000 are tightly entwined at the operating system level. Exchange 2000 uses Active Directory to hold user and mailbox information, thus removing the requirement to run two directory services. When you have Exchange 5.5 in your environment, it becomes necessary to keep the Exchange 5.5 directory and Active Directory in synchronization.

This is usually the first step to take before migrating the Exchange 5.5 servers to Exchange 2000. Synchronizing the two directories ensures that any changes made to the Exchange directory are correctly reflected in Active Directory and vice versa. However, you must plan for the connection between Windows 2000 Active Directory and the Exchange directory. This is because Active Directory does not contain the necessary objects and fields within the schema to hold the additional information required to ensure complete fidelity of information between the two directories.

Architecture and Design Phases

The creation of a connection between Exchange 5.5 and Active Directory has the following phases:

- Plan and deploy Active Directory
- Review Exchange 5.5 environment

- Plan for and design installation of Active Directory Connector
- Plan for extending Active Directory Schema and Prepare Forest
- Plan for preparing Windows 2000 Domain

Before looking at each of these in detail, the design considerations and prerequisites should be addressed.

By now you should have deployed your Active Directory design and worked out how this will be integrated into your network infrastructure. This chapter does not cover the planning of this base Active Directory deployment. It does contain the extra things you need to plan for to upgrade from Exchange 5.5 to Exchange 2000.

You should have a thorough and, preferably documented, understanding of your Exchange 5.5 architecture, site topology, server domain affinity and related topics.

Windows 2000 Active Directory

You should have already installed Windows 2000 Server or Advanced Server and set up Active Directory by running the Active Directory Installation Wizard (DCPROMO.EXE) on the Windows 2000 domain controllers. The Windows 2000 environment must be stabilized before connecting Active Directory to Exchange 5.5.

For more information on the procedures for installing Windows 2000 and promoting servers to domain controllers, see the following document:

http://www.microsoft.com/windows2000/library/planning/server/serversteps.asp

To begin, the Windows 2000 environment can be in either Native or Mixed mode. However, Windows 2000 Native Mode allows the creation of Universal Security Groups, which can only exist in Native mode. Exchange 2000 uses these for applying permissions to public folders, where Exchange 5.5 uses Distribution Lists. Although Distribution Groups exist within Windows 2000, they can be used only for sending mail and not as security principals. A distribution group can be converted to a security group in Native mode only.

In situations where migrating the target domain to native mode is not possible or practical in the timescales required, it is recommended that Exchange 2000 be installed into a Native mode child domain, or at least that the Active Directory Connector be configured such that Distribution Lists are created in a Native Mode domain.

Resource Requirements

As you saw in Chapter 3, “System Dependencies”, the resource

requirements for an Exchange 2000 rollout can be quite large. This section quickly reviews the areas that apply to this chapter:

- Personnel
- Security and Account Privileges
- Skills
- Hardware, Software and Logistics

Personnel

Depending on the size of your company, the deployment of Exchange 2000 can be a cooperative effort. If you are a LIC, LIO, LNC or even a MNO where you have a degree of specialization within your IT department, you need to coordinate between teams. Specifically, you need to ensure liaison between the messaging team and the infrastructure, network administration and DNS teams. It is critical that the tasks in this chapter be executed with the full cooperation of these teams.

With Exchange 5.5, having separate messaging and network administration teams did not critically affect the performance of each component or either infrastructure. However, the lines between these two teams blur significantly with the advent of Windows 2000 and Exchange 2000. So now is the time to take your counterparts out to lunch, ask how the family is doing, and generally act interested in the other person. If the Exchange 5.5 system needs to be connected to Active Directory, the messaging administrator and the network administrator must be joined at the hip.

Security and Account Privileges

In order to carry out most of the plans discussed here, you will need to be logged on with an account that has the following Windows 2000 account privileges:

- Schema Administrator
- Domain Administrator
- Enterprise Administrator

The account you use should also have the following privileges or roles outside the Active Directory:

- Windows 2000 Domain Administrator
- Exchange 5.5 Permissions Admin

In addition, you must have knowledge of the Exchange 5.5 Service Account name and password. These requirements are covered in Chapter 2, “Configuring Active Directory for Exchange 2000”.

If you are entrusted with connecting the Exchange 5.5 system with Active

Directory (and you did not take your Active Directory Network Administrator to lunch), you will need the network administrator to be physically present during the deployment of Exchange 2000.

Skills

To carry out the procedures in this chapter, you should have a working understanding of Windows 2000 Active Directory, Organizational Unit (OU) structure and Exchange 5.5.

Hardware, Software and Logistics

Ideally, you should have physical access to your Exchange 5.5 servers and at least one of each of your Windows 2000 Domain Controllers for all the domains in your forest. You will also require the following software:

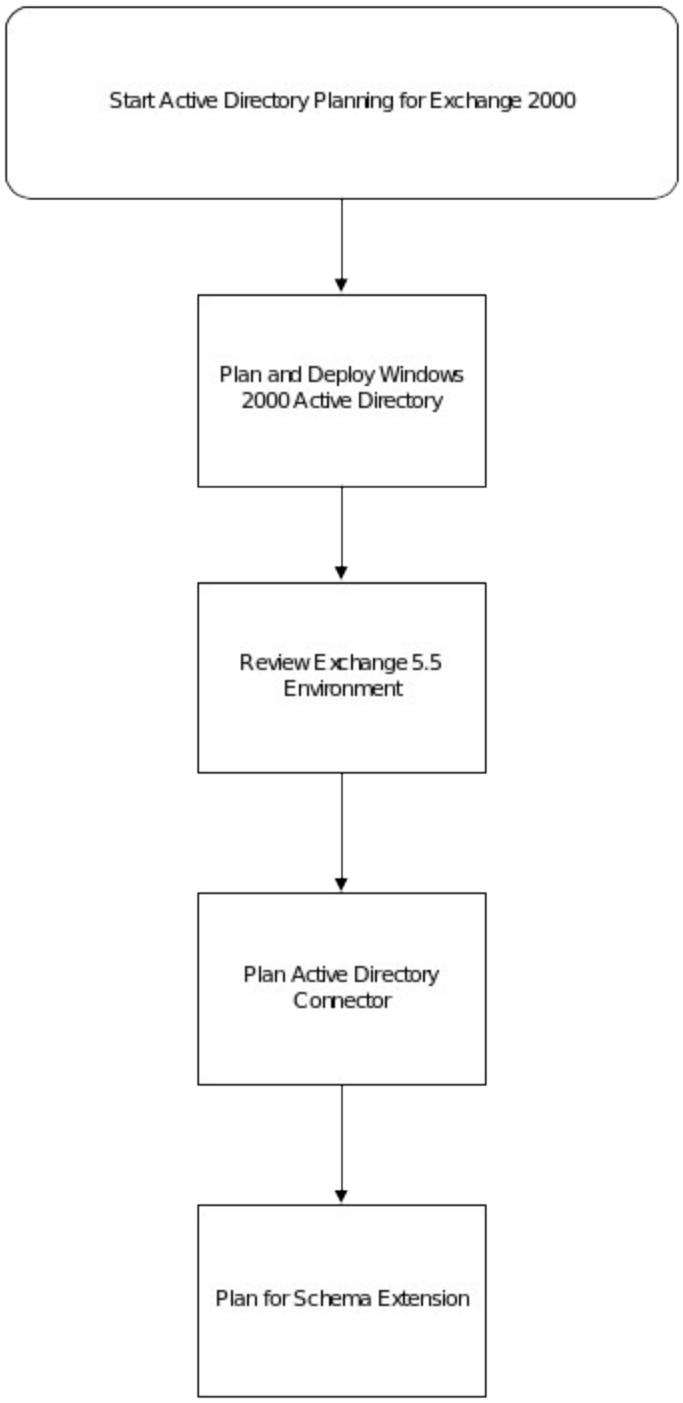
- Exchange 2000 Server CD
- Windows 2000 Server or Advanced Server CD
- Windows 2000 Service Pack 1 CD
- DCDIAG.EXE from the Support Tools on the Windows 2000 CD.
- AD Sizer from the Microsoft web site.

Planning Prerequisites

Before you undertake this procedure, perform the following actions:

- Deploy a fully functional Active Directory.
- Deploy a fully functional DNS environment
- Ensure that all your Exchange 5.5 servers are members of a Windows 2000 domain.
- Understand the system dependencies highlighted in the “Windows 2000 Dependencies” and “Exchange 5.5 Dependencies” sections in Chapter 3 of the Architecture guide.

PLANNING FOR ACTIVE DIRECTORY


Start Active Directory Planning for Exchange 2000
Plan and Deploy Windows 2000 Active Directory
Review Exchange 5.5 Environment
Plan Active Directory Connector
Plan for Schema Extension

A solid Windows 2000 Active Directory architecture is essential for the successful execution of an Exchange 2000 architecture plan. The operating system and network architecture must be stable and functional before the Exchange 2000 messaging architecture is laid on top of it.

It is prudent to measure the baseline performance of your Windows 2000

and networking environment while your are designing your Exchange 2000 environment. This would be a good time to remove those nagging kinks in the underlying plumbing and to ensure that your underlying structure is performing correctly.

A good description of Active Directory and how it interacts with Exchange is available in Chapter 5 of Microsoft Exchange 2000 Server Planning and Installation. A good case study of the planning and deployment process is also available.

Figure 1 gives you a detailed roadmap of the required planning steps.

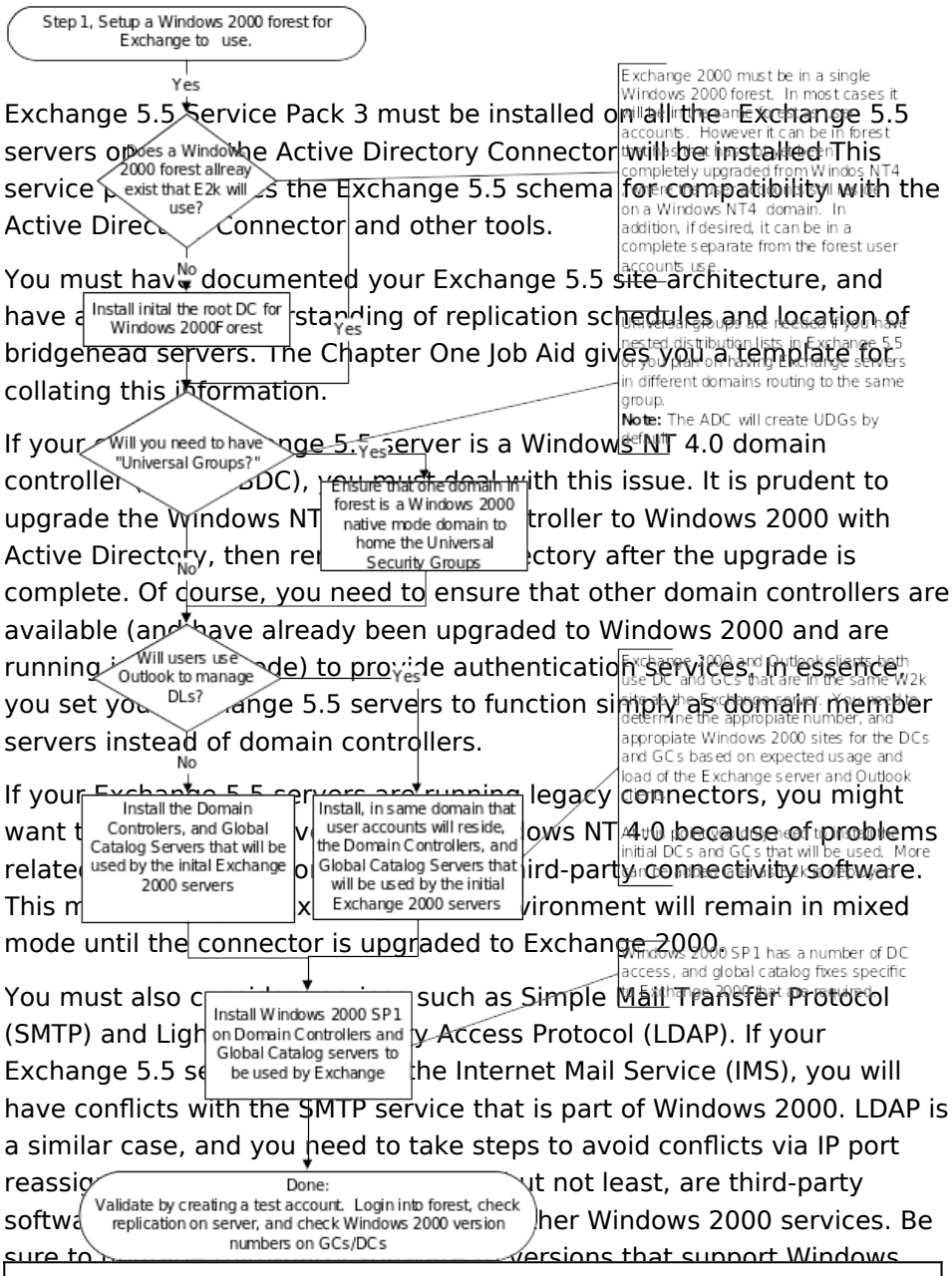

Step 1, Setup a Windows 2000 forest for Exchange to use.
Yes
Does a Windows 2000 forest allreay exist that E2k will use?
No
Install inital the root DC for Windows 2000Forest
Yes
Will you need to have "Universal Groups?"
Yes
Ensure that one domain in forest is a Windows 2000 native mode domain to home the Universal Security Groups
No
Will users use Outlook to manage DLs?
Yes
No
Install the Domain Controlers, and Global Catalog Servers that will be used by the inital Exchange 2000 servers
Install, in same domain that user accounts will reside, the Domain Controllers, and Global Catalog Servers that will be used by the initial Exchange 2000 servers
Install Windows 2000 SP1 on Domain Controllers and Global Catalog servers to be used by Exchange
Done:
Validate by creating a test account. Login into forest, check replication on server, and check Windows 2000 version numbers on GCs/DCs
Exchange 2000 must be in a single Windows 2000 forest. In most cases it will be in the same forest as user accounts. However it can be in forest that is not installed or completely upgraded from Windos NT4 domains. In addition, if desired, it can be in a complete separate from the forest user accounts use.
Universal groups are needed if you have nested distribution lists in Exchange 5.5 or you plan on having Exchange servers in different domains routing to the same group.
Note: The ADC will create UDGs by default.
Exchange 2000 and Outlook clients both use DC and GCs that are in the same W2k site as the Exchange server. You need to determine the appropiate number, and appropiate Windows 2000 sites for the DCs and GCs based on expected usage and load of the Exchange server and Outlook users.
At a minimum you need to upgrade initial DCs and GCs that will be used. More information can be found in
Windows 2000 SP1 has a number of DC access, and global catalog fixes specific to Exchange 2000 that are required

Figure 1 - Prepare Windows 2000 for Exchange 2000

Exchange 5.5 Service Pack 3 must be installed on all the Exchange 5.5 servers on the Active Directory Connector will be installed This service p es the Exchange 5.5 schema for compatibility with the Active Direc Connector and other tools.

You must have documented your Exchange 5.5 site architecture, and have a rstanding of replication schedules and location of bridgehead servers. The Chapter One Job Aid gives you a template for collating this information.

If your nge 5.5 server is a Windows NT 4.0 domain controller (BDC), you must deal with this issue. It is prudent to upgrade the Windows NT troller to Windows 2000 with Active Directory, then re ectory after the upgrade is complete. Of course, you need to ensure that other domain controllers are available (and have already been upgraded to Windows 2000 and are running i ode) to provide authentication services. In essence you set yo nge 5.5 servers to function simply as domain member servers instead of domain controllers.

If your Exchange 5.5 servers are running legacy connectors, you might want t v ows NT 4.0 because of problems relate o ird-party connectivity software. This m x vironment will remain in mixed mode until the connector is upgraded to Exchange 2000.

You must also c such as Simple Mail Transfer Protocol (SMTP) and Ligh y Access Protocol (LDAP). If your Exchange 5.5 se he Internet Mail Service (IMS), you will have conflicts with the SMTP service that is part of Windows 2000. LDAP is a similar case, and you need to take steps to avoid conflicts via IP port reassig t not least, are third-party softwa her Windows 2000 services. Be sure to versions that support Windows

Exchange 5.5 to Active Directory. The ADC can replicate objects in the Windows 2000 Active Directory into the Exchange Server 5.5 directory and vice-versa. When you have already deployed Exchange 5.5 and are thinking of deploying Active Directory, use replication to aid in the population of Active Directory with the rich information already available

in Exchange 5.5. This is a necessary stage for achieving coexistence between Exchange Server 5.5 and Exchange 2000 Server.

In the future, ADC technology might be extended to support replication of other directories, such as Netscape Directory Server, DCL X.500, generic LDAP directories, and other Windows 2000 Active Directories.

How ADC Works

ADC works in the following ways:

- Uses the LDAP application programming interface (API) to perform fast replication between the two directories
- Hosts all active replication components on Active Directory, not on the foreign system
- Replicates only changes between the two directories whenever possible
- Maintains object fidelity through replication (for example, the Active Directory Group object maps to the Exchange Distribution List object)
- Hosts multiple connections on a single Active Directory server and manages these using Connection Agreements.

Be aware that ADC is not seen a long-term solution for linking Active Directory and Exchange 5.5.

ADC Versions

There are two versions of the ADC: the Windows 2000 version, and the Exchange 2000 version. Although a version of ADC that provides the basic replication functionality comes with Windows 2000, you need the one included with Exchange 2000.

- **Windows 2000 ADC** – The version of ADC included in Windows 2000 replicates directory information in Exchange 5.5 to Active Directory and vice versa. You have already invested heavily in the Exchange directory, and much of this data can be uploaded in bulk to Active Directory, which decreases implementation time. Through replication, the Active Directory administrator can also perform basic management functions for Exchange 5.5 users.
- **Exchange 2000 Server ADC** – The Exchange 2000 Server ADC update is an enhanced connector included with Exchange 2000 Server. Whereas the Windows 2000 ADC simply replicates objects in the Exchange site-naming context (for example, Recipients containers) to Active Directory, the Exchange 2000 ADC also replicates data from the configuration-naming context, thus

providing support for mixed-vintage Exchange sites and downstream routing.

The upgrade path between the two versions of ADC is seamless. You can deploy Windows 2000 ADC to build the basic Active Directory very quickly, and when ready, you can install the updated ADC when installing your first Exchange 2000 Server.

Architecture Strategy

Depending upon your existing Active Directory and Exchange 5.5 architecture, there are several ways you can design the connection between the two directories. Chapter 16 of the Microsoft Exchange 2000 Server Planning and Installation provides a detailed analysis of the pros and cons for each strategy. Chapter 20 of the Windows 2000 Deployment Planning Guide provides additional information on various strategies.

Figure 2 and Figure 3 are the detailed roadmap you can use to plan for implementing the Active Directory Connector.

Preview Documentation

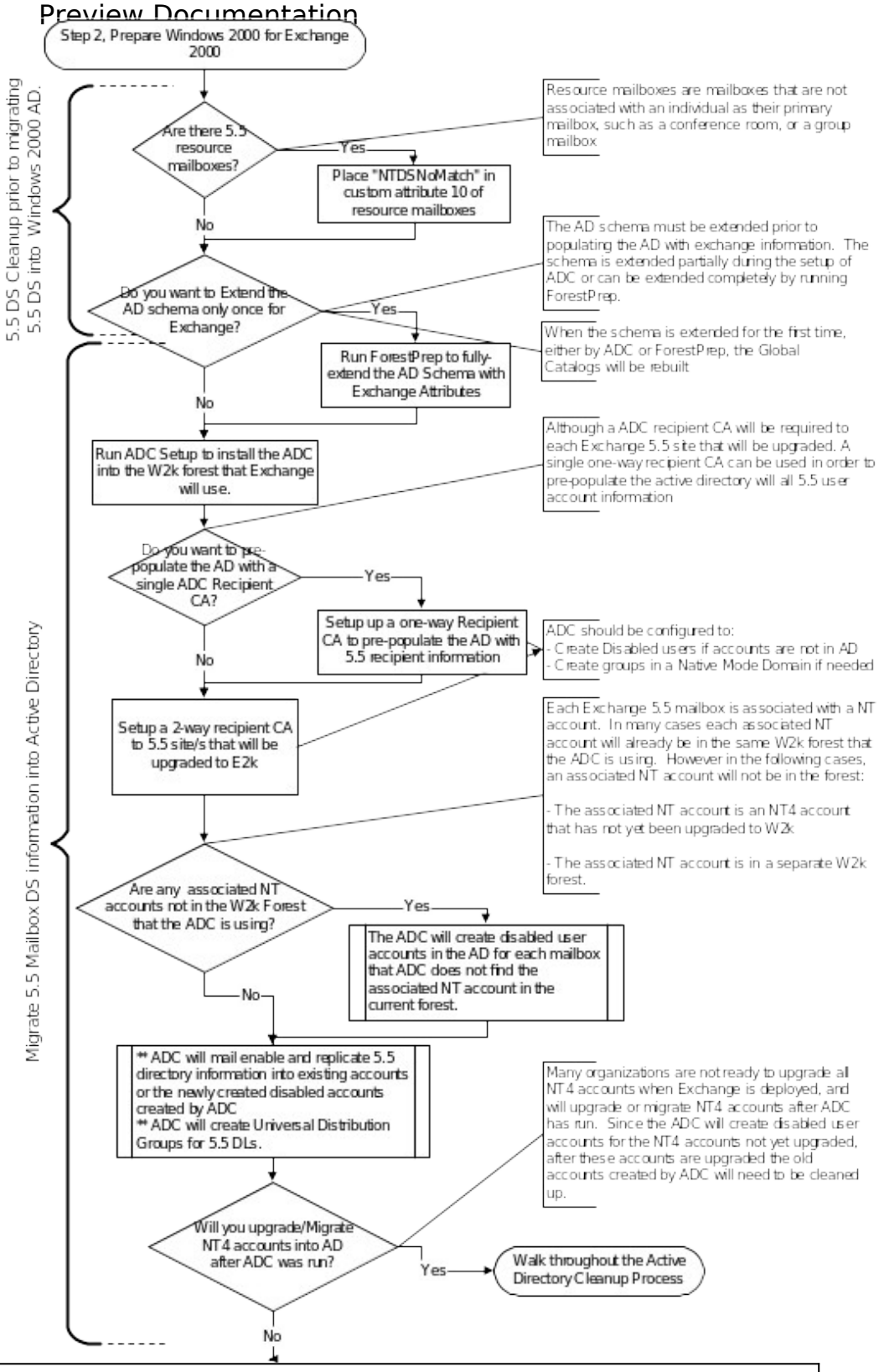

Step 2, Prepare Windows 2000 for Exchange 2000
5.5 DS Cleanup prior to migrating 5.5 DS into Windows 2000 AD.
Migrate 5.5 Mailbox DS information into Active Directory
Are there 5.5 resource mailboxes?
Yes
Place "NTDSNoMatch" in custom attribute 10 of resource mailboxes
No
Resource mailboxes are mailboxes that are not associated with an individual as their primary mailbox, such as a conference room, or a group mailbox
Do you want to Extend the AD schema only once for Exchange?
Yes
Run ForestPrep to fully-extend the AD Schema with Exchange Attributes
No
The AD schema must be extended prior to populating the AD with exchange information. The schema is extended partially during the setup of ADC or can be extended completely by running ForestPrep.
When the schema is extended for the first time, either by ADC or ForestPrep, the Global Catalogs will be rebuilt
Run ADC Setup to install the ADC into the W2k forest that Exchange will use.
Do you want to pre-populate the AD with a single ADC Recipient CA?
Yes
Setup up a one-way Recipient CA to pre-populate the AD with 5.5 recipient information
No
Although a ADC recipient CA will be required to each Exchange 5.5 site that will be upgraded. A single one-way recipient CA can be used in order to pre-populate the active directory will all 5.5 user account information
ADC should be configured to:
- Create Disabled users if accounts are not in AD
- Create groups in a Native Mode Domain if needed
Setup a 2-way recipient CA to 5.5 site/s that will be upgraded to E2k
Each Exchange 5.5 mailbox is associated with a NT account. In many cases each associated NT account will already be in the same W2k forest that the ADC is using. However in the following cases, an associated NT account will not be in the forest:
- The associated NT account is an NT4 account that has not yet been upgraded to W2k
- The associated NT account is in a separate W2k forest.
Are any associated NT accounts not in the W2k Forest that the ADC is using?
Yes
The ADC will create disabled user accounts in the AD for each mailbox that ADC does not find the associated NT account in the current forest.
No
** ADC will mail enable and replicate 5.5 directory information into existing accounts or the newly created disabled accounts created by ADC
** ADC will create Universal Distribution Groups for 5.5 DLs.
Will you upgrade/Migrate NT4 accounts into AD after ADC was run?
Yes
Walk throughout the Active Directory Cleanup Process
Many organizations are not ready to upgrade all NT4 accounts when Exchange is deployed, and will upgrade or migrate NT4 accounts after ADC has run. Since the ADC will create disabled user accounts for the NT4 accounts not yet upgraded, after these accounts are upgraded the old accounts created by ADC will need to be cleaned up.
No

Figure 2 - Architect Active Directory Connector

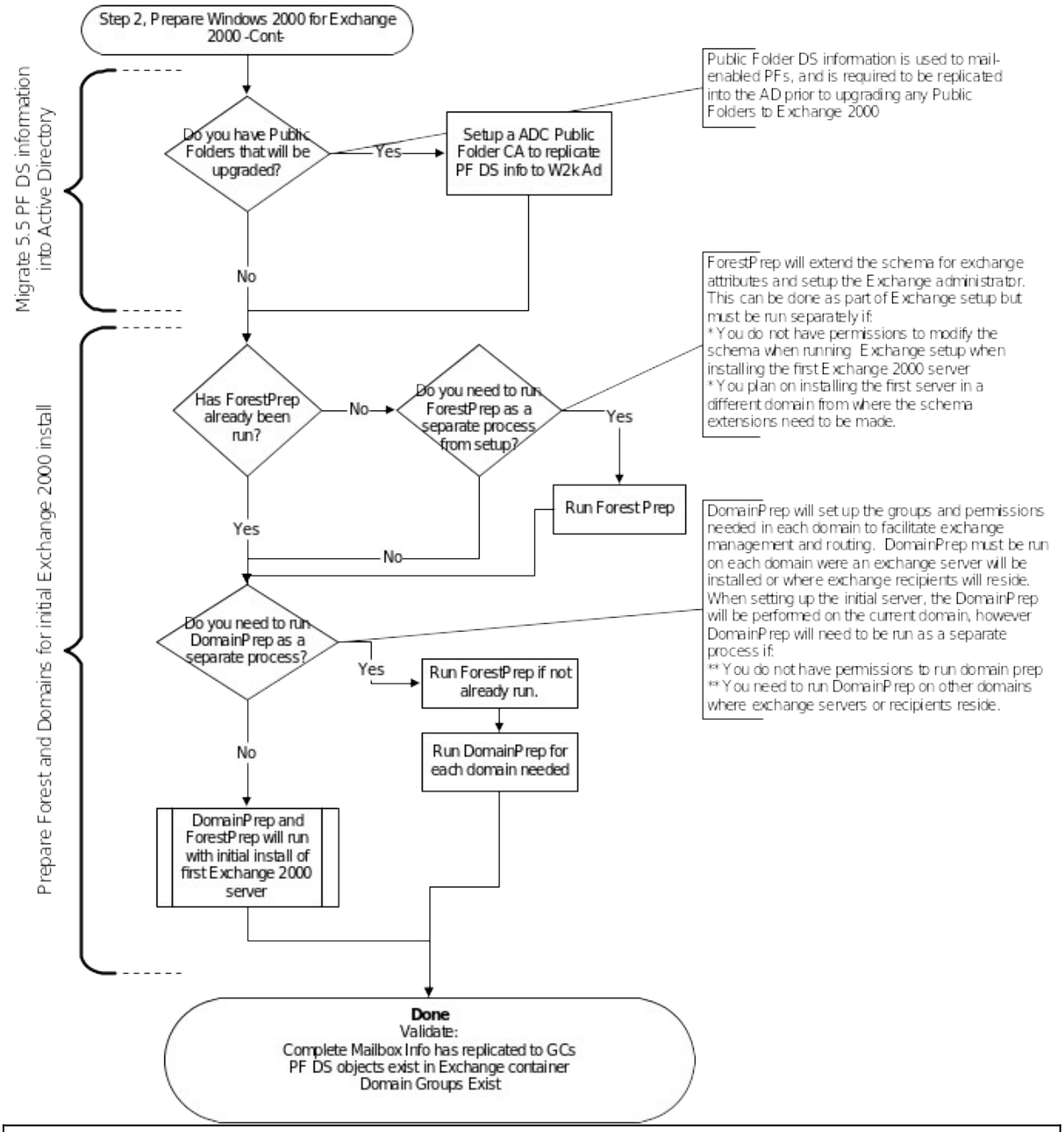

Step 2, Prepare Windows 2000 for Exchange 2000 -Cont-
Migrate 5.5 PF DS information into Active Directory
Do you have Public Folders that will be upgraded?
Yes
Setup a ADC Public Folder CA to replicate PF DS info to W2k Ad
Public Folder DS information is used to mail-enabled PFs, and is required to be replicated into the AD prior to upgrading any Public Folders to Exchange 2000
No
Prepare Forest and Domains for initial Exchange 2000 install
Has ForestPrep already been run?
No
Do you need to run ForestPrep as a separate process from setup?
Yes
ForestPrep will extend the schema for exchange attributes and setup the Exchange administrator. This can be done as part of Exchange setup but must be run separately if:
* You do not have permissions to modify the schema when running Exchange setup when installing the first Exchange 2000 server
* You plan on installing the first server in a different domain from where the schema extensions need to be made.
Run Forest Prep
Yes
No
Do you need to run DomainPrep as a separate process?
Yes
Run ForestPrep if not already run.
Run DomainPrep for each domain needed
No
DomainPrep and ForestPrep will run with initial install of first Exchange 2000 server
DomainPrep will set up the groups and permissions needed in each domain to facilitate exchange management and routing. DomainPrep must be run on each domain were an exchange server will be installed or where exchange recipients will reside. When setting up the initial server, the DomainPrep will be performed on the current domain, however DomainPrep will need to be run as a separate process if:
** You do not have permissions to run domain prep
** You need to run DomainPrep on other domains where exchange servers or recipients reside.
Done
Validate:
Complete Mailbox Info has replicated to GCs
PF DS objects exist in Exchange container
Domain Groups Exist

Figure 3 - Architect Active Directory Connector (contd.)

PLAN FOR SCHEMA EXTENSION

Related Topics

Exchange 2000 Server and Active Directory – TechNet article

Exchange 2000 Migration: Deploying the Active Directory Connector Within Microsoft

Description of the Active Directory Connector Schema Map

Remember that the Active Directory schema will get extended at various stages – once during the installation of the Active Directory Connector, and again during the installation of Exchange. Schema extensions have several ramifications of which you should be aware:

- They are not reversible.
- They will generate network traffic.
- Your Global Catalog will be rebuilt.

Unless you are a Schema Administrator, you will not be able to extend the schema. This means that the installation of the ADC and running part of the Exchange 2000 setup requires you to have Schema Administrator privileges or the full co-operation of the person who is the Schema Administrator in your environment. Please refer to Chapter 2 of the Deployment Guide for more details on the privileges needed to extend the schema.

You should also plan for the replication traffic generated by the large number (in excess of 1,000) changes to the schema triggered by the Exchange 2000 and Active Directory Connector setup. Schema updates affect the entire forest, and depending on the size of the directory and network topology, may take a considerable amount of time.

In this chapter, you covered how to prepare the Windows 2000 Active Directory to support the deployment of Exchange 2000. In addition to ensuring a solid Windows 2000 Active Directory, additional steps include preparing the forest by extending the schema to hold additional objects and attributes.

To implement the changes that you have planned in this document, you should see Chapter 2, “Configuring Active Directory for Exchange 2000” in the Deployment section.